Plaintiffs' Exhibit 63

Privacy Off-Site - Template

Inventory of Status Quo

What are we doing that's good (perceived or real) from a privacy perspective? List everything with a brief description of each.

Product

Granular Data Permissions
-Applications must get explicit authorization from the user before accessing anything more than publicly available information
-Once authorized, applications can only access those pieces of data approved by the user
-Came out of OPC investigation and fits with "just-in-time" consent model outlined by FTC

Privacy Settings
-Applications are subject to same privacy settings as users
-Relatively clear and simple opt-out for both Platform and Instant Personalization
-Ability to block and/or report applications that may be misbehaving
-Settings for information accessible to friends' applications

Social Plugins
-Allow websites to provide social experiences without sharing any data with third parties
-Positioned this as a privacy innovation at launch, but confusion and backlash from Instant Personalization made message less effective

Instant Personalization
-For recent integrations, we've spent a lot of time making the disclosures on partners sites clear and prominent, with easy ability to opt out

Per Object Privacy for Applications
-Allows apps access to the same tool we provide in our own publisher for posts made through the app (http://developers.facebook.com/blog/post/362)

Policy and Enforcement

-On a high level, we require developers to offer choice and control, provide experiences that are in-line with user expectations, and abide by our SRR
-We require all applications to have a privacy policy and to link to it both in the GDP dialog (required by OPC and FTC) and on the canvas page
-We require applications to only make requests for data needed to provide the

experience
-We prohibit applications from sharing Facebook data with specified fourth parties
-We review applications reported by users or flagged by automated systems and take action according to our policies; action ranges from placing a moratorium on distribution channels to disabling the application and removing all content created through it, and we've disabled thousands of applications for violating our policies

Communications/Strategy

-When we lead with the value proposition and can demonstrate it clearly, we win (examples: recent IP launches for Bing, Rotten Tomatoes, and to a lesser extent, Scribd; single sign-on for mobile); being confident in the message and promoting it through launch events, etc. helps

What are we doing that's bad (perceived or real) from a privacy perspective?

Product

Granular Data Permissions
-Viewed as a failure from a product perspective because it deters app usage (example: NYT and its scarily long GDP dialog: http://nyti.ms/gr4bII). We're exploring options to replace it, one of which is a redesigned registration dialog for Connect that displays the exact information you're providing in a pre-filled, editable form.

Friends' Data
-By default, applications can access friends' data (birthday, status updates, photos, videos, etc.) if they get authorization from the end user
-There's no consistency in how we set defaults for new classes of data (example: when we launched Places, we checked the box that allows friends' apps to access your check-ins if you had at least two of the 17 other boxes already checked).

Social Plugins and Connect
-Confusing experience: Users aren't sure what data is being shared, or what happens after they click; lots of different blue buttons across the web with little explanation of the consequences/value proposition
-Don't have a good answer to the question of what passive data we collect when people land on sites with social plugins or Connect

Instant Personalization
-Sharing personal data with third parties without user consent

Read vs. Write Access
-We treat the ability to access a user's data and the ability to act on a user's behalf (post to the profile, etc.) as equal permissions; however, users view them as very different

Connecting Accounts
-Through email hashes, we help partners connect accounts on their sites with Facebook accounts, sometimes before the person even explicitly connects

Policy and Enforcement

-There's no approval process for new applications. As long as you have a Facebook account, you can get an API key. Also, when registering an application, "Privacy Policy" is not a required field (though we do include a reminder that it's required by our FPP).
-Enforcement is imperfect. For example, there's no way for us to enforce the requirement that apps only request data they need to function, as it would require too many ops resources and overly burden developers whose applications are quickly evolving, and who don't want to have to ask for new permissions each time they make a change.
-Difficult to impossible to enforce our requirement that applications not share Facebook data with specified fourth parties

Data Portability

-No consistent point-of-view and special relationships with partners that undermine larger philosophical arguments (example: recent back-and-forth with Google over exporting friends' contact info); need to decide if we're going to be principled or pragmatic (can't be both)

Organization

-Lack of ownership over privacy means that we don't have a good understanding of where we are or a clear vision for where we're going (examples: cycles spent figuring out the UID issue, what we track through the Like button, why we keep data and for how long, etc.)
-We allow lots of functionality because we want Platform to be open and believe that developers will ultimately find uses for it; however, this makes us vulnerable to criticism
-We err on the side of making it easy for the developer rather than intuitive for the user

What are our competitors (e.g. Google, Twitter) and other companies doing in this space and how do we compare?

N.B. We're the only major player in the social platform space, and this is likely to continue for the foreseeable future.

Google
-Most popular APIs don't come close to ours in terms of volume of usage. They also don't involve social or personal information (Maps API, for example). This makes them less vulnerable to privacy criticism, but also less powerful.
-OpenSocial and FriendConnect were never widely adopted and, for all intents and purposes, no longer exist.
-An analogous platform for Google would be one that provides access to search and ad data (the core parts of the service). Google has been very effective at painting us into a corner on data portability (positioning our platform as closed), while at the same time refusing to answer the question of why it doesn't provide a search or ads API.

Twitter
-Over 100,000 apps responsible for 75% of all traffic and 60% of all tweets
-Service is different in that everything is public by default, and thus there's no user expectation of privacy
-Not much diversity in apps: Most simply provide an easier way to either consume or publish content. At launch, most apps focused on filling feature holes that the company had yet to tackle (for example, TwitPics and mobile Twitter apps). As the company has matured, many of these feature holes have been filled, and development has shifted to three main areas: meme trackers, real-time communication, and business/competitive intelligence.

Apple
-App Store has 300,000 applications.
-Mentioned most often as a counterpoint to our open approach; all applications are subject to approval by Apple, outlined in the iPhone SDK agreement, and an NDA forbids developers from disclosing their rejection notices. Apps are screened for both functional and content violations

What could/should we be doing differently, either to correct existing problems or to improve our positions in the future?

Product

Granular Data Permission
-Change the UI to strike a better balance between scaring people and providing useful and comprehensive disclosure (new Connect reg form referenced above is one idea)

Apps Dashboard
-If person hasn't used an application in a long time, automatically remove it (i.e. make session expire)
-Include applications your friends use that have accessed your information
-Provide the ability to opt in to notifications when applications access data or certain types of data

Friends' Data
-Only allow applications to access friends' public data, since the vast majority don't need anything more to work. Whitelist those that do.

Instant Personalization
-Develop a UI that serves as a persistent reminder that your experience on the partner site is being powered by Facebook

Social Plugins and Connect
-Improve the UI so that people have a better understanding of what happens after clicking the blue button. This is good from a product standpoint as well because it helps the user understand the value proposition.

Policy and Enforcement

-Anything that improves our enforcement story - particularly for the long tail of developers - and lessens the perception of Platform as the "Wild West"
-Run a script to identify those applications that don't have privacy policies and email the developers

Communications/Strategy

-Figure out where we want to take a strong stance because we're doing better than others and be vocal about it (for example, the hypocrisy of news outlets that share registrants' personal data with third parties, but then criticize us for things like unintentionally passing UIDs in referrers)
-Continue to focus our message on the value provided to users
-Continue to choose partners and implementations where social makes sense (e.g. review sites like Yelp and Rotten Tomatoes)

Organization

-Establish ownership over privacy so that we can better understand status quo and develop a clear position moving forward
-Audit Platform for potential additional privacy landmines (like the UID issue, tracking through social plugins, etc.)

Parameters

What changes (if any) to our current practices have been or are likely to be proposed that should be declared off-limits? Consider proposals emanating from internal and external sources.

-Restrictions on the use of cookies: Cookies are a critical piece of the technology that allows people to carry their identity and connections with them around the web
-Shut down instant personalization: Our vision for the future is for the web to be social by default, and this would be a serious hit to that vision

Global Perspective

How are our current practices viewed by users and regulators outside of the United States?

N.B. The rest of the world is behind the U.S. on this issue, and Canada helped provide some additional cover. As a result, views are largely the same internationally with several exceptions.

-Third-party cookies: There has been a move in the EU to require third parties to ask explicit consent to place cookies when these are not for the domain of the primary website. This was aimed at third-party ad networks primarily but could equally apply to all Facebook apps. It is still being worked out so the full impact isn't yet known. Some outcomes would mean that apps and any ad networks they use would have to ask permission before installing cookies.

-Ad networks: There is a lot of regulatory concern about ad networks. Where apps use these, the concern may be heightened, as there is a chance for ad network OBA data to be combined with Facebook data.

-Location data: This is especially sensitive in the EU. Most people are happy that

Places has appropriate controls in place. However, some of the location-based apps using Facebook APIs could be a lot more "on the edge" in regulatory terms. We need to consider how much freedom we want to give them as the blame for bad practices may be brought back to Facebook.

-"Bad" speech accessible via the API: There have been instances of people using the API to find hate speech and other bad content in public posts. This could grow as an issue with public authorities using Platform to identify potentially illegal content en masse and asking us to move against it. This carries significant privacy implications for our users who may be shocked to find their Facebook data accessed in this way.

What steps (if any) should we take to better align our practices with global expectations?

Because the rest of the world (with the exception of Canada) hasn't been following Platform as closely, in general, anything we do to improve our position in the U.S. will be beneficial elsewhere as well.